Are my Apps Peeking? Comparing Nudging Mechanisms to Raise Awareness of Access to Mobile Front-facing Camera

Mariam Hassib
mariam.hassib@unibw.de
Bundeswehr University
Munich, Germany

Hatem Abdelmoteleb
hatem.r.abdelmoteleb@gmail.com
German University in Cairo
Cairo, Egypt

Mohamed Khamis
mohamed.khamis@glasgow.ac.uk
University of Glasgow
Glasgow, United Kingdom

ABSTRACT

Mobile applications that are granted permission to access the device's camera can access it at any time without necessarily showing the camera feed to the user or communicating that it is being used. This lack of transparency raises privacy concerns, which are exacerbated by the increased adoption of applications that leverage front-facing cameras. Through a focus group we identified three promising approaches for nudging the user that the camera is being accessed, namely: notification bar, frame, and camera preview. We experimented with accompanying each nudging method with vibrotactile and audio feedback. Results from a user study (N=15) show that while using frame nudges is the least annoying and interrupting, but was less understandable than the camera feed and notifications. On the other hand, participants found that indicating camera usage by showing its feed or by using notifications is easy to understand. We discuss how these nudges raise user awareness and the effects on app usage and perception.

CCS CONCEPTS

• **Human-centered computing** → **Mobile computing**; **Mobile devices**; • **Security and privacy** → **Human and societal aspects of security and privacy**.

KEYWORDS

Privacy, Mobile Devices, front-facing camera

ACM Reference Format:
Mariam Hassib, Hatem Abdelmoteleb, and Mohamed Khamis. 2020. Are my Apps Peeking? Comparing Nudging Mechanisms to Raise Awareness of Access to Mobile Front-facing Camera. In *19th International Conference on Mobile and Ubiquitous Multimedia (MUM 2020), November 22–25, 2020, Essen, Germany*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3428361.3428384

1 INTRODUCTION

Before using mobile/desktop applications, users are often provided with privacy notices. It is well established that these notices are of little effect in raising user awareness of what is actually being tracked from their data [20, 24, 30]. While mobile applications request access to resources before using them, research has shown that users do not fully understand applications' capabilities and what they can do with the user's data [20]. For example, a common misconception about camera permissions on Android and iOS devices is that the camera is never accessed unless its feed is shown to the user [19]. Android 10 limits the access of apps to system resources to occasions where the app is being used, while iOS presents the same option among multiple settings. Still, these features do not prevent the mobile application with permission to access the camera from retrieving the camera feed at any time during the app's usage without notifying the user [4, 15]. This means that users are often unaware of the authority given to mobile applications [1]. This issue raises privacy concerns and violates one of the basic guidelines for secure interaction design because users no longer posses accurate awareness of mobile applications' authority [35].

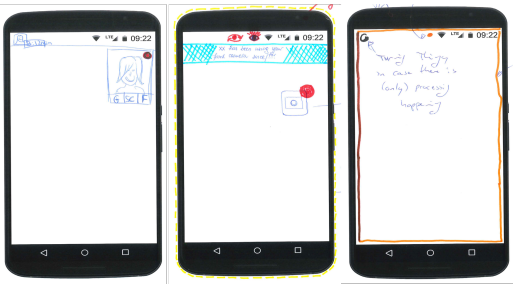

Figure 1: Three designs from our focus group: Camera feed on top corner with a red recording dot and the apps using it (left); floating camera icon with red recording dot and notification bar with app name (middle); and Red/Orange frame showing camera access/processing (right).

This problem is amplified in case of front-facing cameras; the availability of depth cameras and the increasing processing power of mobile devices are leading to a surge of mobile apps that leverage said cameras [18]. These include social media applications (e.g., Snapchat), security applications (e.g., facial recognition), facial expression identification from images and videos [10, 32, 36], cognitive stress detection [25], and further input/navigation mechanisms [22]. While these applications bring benefits to the user, they also present a threat as sensitive information can be retrieved if the data is not adequately handled, such as mental states [16], visual interests [18], and emotions [10].

In this work, we design and compare three approaches for nudging users when the front-facing camera is accessed by an application. Our goal is to make the front-facing camera's usage transparent to users. To this end, we report on results of a focus group through which we identified promising nudging approaches. We then evaluated our prototype implementations in a user study (N=15) in which we collected subjective feedback about the proposed techniques when used with three types of feedback: vibration, sound and combination of both. Our results show that using blinking frames to

MUM 2020, November 22–25, 2020, Essen, Germany
© 2020 Copyright held by the owner/author(s). Publication rights licensed to ACM. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *19th International Conference on Mobile and Ubiquitous Multimedia (MUM 2020), November 22–25, 2020, Essen, Germany*, https://doi.org/10.1145/3428361.3428384.

communicate camera usage does not interrupt users and remains noticeable. However, showing the camera feed or displaying notifications to indicate camera usage are more understandable by users. We discuss the potential implications of increasing the awareness and the transparency of front-facing camera usage.

The main **contribution** of this work is the design and evaluation of techniques for nudging the user that the front-facing camera's feed is being accessed by an application.

2 BACKGROUND AND RELATED WORK

2.1 Front Camera Usage

Front-facing cameras are widely used in market applications and in the research domain. Games and entertainment applications utilize them for gesture input, facial tracking, or eye-based input to adapt and control the gaming environment [7, 9, 13, 27, 29]. The most prominent use of front-facing cameras is enabling video chatting on the go, and allowing social media applications to send photos, overlay images and use filters and backgrounds (e.g., Facebook, Snapchat and Instagram). There are countless applications available on the Google and iPhone application stores which provide filters and overlays over the users' face (e.g. *Face Changer Camera* [33]) which all require access to the front-facing camera.

2.2 Privacy Nudges on Smartphones

Users often do not understand permissions they give to Android applications [11]. In cases where they do, they are often unsure about the threats arising from apps requesting too many permissions [17]. A body of work investigated how to support users' awareness of the permissions they are giving and potential risks of doing so.

One direction is to use privacy nudges to alert users of the privacy implications of app permissions. Acquisti et al. explored how nudges are used for privacy and security [1]. On mobile platforms, most research was concerned with location privacy on mobile platforms [2, 3, 6, 8]. Aiming to remind users of application permissions and encouraging users to re-consider them, Almuhimedi et al. conducted a field study on daily nudges which show users the frequency their mobile applications access sensitive location data [2]. Their results show that this motivates users to review permission settings [2]. Balebako et al. [6] developed two types of interfaces: just-in-time notifications that are shown the moment data is shared and a visualization which summarizes shared data. Alrayes et al. [3] developed a location feedback tool. It was designed as a floating icon which indicates the threat level of location privacy. Acquasti et al. explain that nudges can be distinguished into education and feedback: the former educates users before a feature is used, while the latter shows the user feedback when the feature is used. Our investigated mechanisms fall under the second category [1].

Other works focused on improving the permissions page. Liu et al. explored providing users with personalized recommendations for application permission settings [23]. Micallef et al. designed blocking and non-blocking privacy nudges to inform users about application data access and asked users to reconsider permissions [26]. Harbach et al. redesigned the permission page of the Google Play Store to support users in considering risks in giving permissions [12]. Similarly, Hettig et al. [14] redesigned the Android permission requests to show examples on what this app can be allowed to do if granted the permission.

2.3 Contribution Over Previous Work

Compared to prior work, ours is the first to focus on privacy nudges related to the use of front-facing cameras. This is distinct from the large body of work on location-privacy as front-facing cameras allow developers to analyze the user's face and eye movements, which come with significant threats to privacy [18].

3 FOCUS GROUP

To develop our design concept for front-facing camera awareness nudges, we conducted a one-hour focus group to 1) identify current usage scenarios of the phone's front-facing camera, and 2) explore potential designs of privacy nudges to communicate front-facing camera usage. We distinguish two types of camera-usage a) accessing the camera feed (e.g., to take a picture, record and/or a video) and b) processing the current feed (e.g., to overlay components, run facial analysis, or track eye movements). The latter comes with more privacy risks [18].

Our focus group consisted of a discussion then a design session. We recruited 5 participants (3 female, 2 male, 25-30 years old). Participants were a mix of undergraduate and postgraduate students with a background in HCI.

In the discussion session, participants were asked to write down and exchange their opinions regarding privacy for front-facing cameras. They mentioned that they use the front-facing camera for the purpose of unlocking their phone (P5) or for entertainment and games. Participants agreed that they mostly use the front-facing camera for video chatting and social media such as Snapchat. Further, when we asked participants how do they feel about applications which run in the background and use the front-facing camera, we found participants found it creepy (P1), and they do not like being watched (P2). Participants mentioned multiple ideas for nudging mechanisms. For example, using persistent notifications with vibration (P2), or using sound such as a beeping or camera shutter sound (P3, P5). Finally, P4 proposed using a scent or the flash to indicate camera access.

The second part of the focus group was comprised of a design session where participants sketched possible implementations of the awareness nudges on smartphone templates. Participants were asked to sketch as many designs as possible to illustrate their ideas of how to nudge for front-facing camera usage in case of camera *access* or video feed *processing*. Figure 1 shows three different design outcomes. Three participants proposed the recording dot icon to be either on the status bar (cf. 1, middle figure) or on the camera view (cf. 1, left figure). P3 suggested using a colored frame which is continuous as long as the camera is being used and the screen is on (cf. 1, right figure). Two participants suggested providing a timer showing how long the camera has been on. Participants also suggested using external hardware such as a shutter which opens when the camera is accessed. To differentiate accessing camera and processing of photos and videos, P1 suggested using two different icons in the status bar (e.g., an eye icon for accessing the camera and loading icon to indicate processing). Furthermore, P4

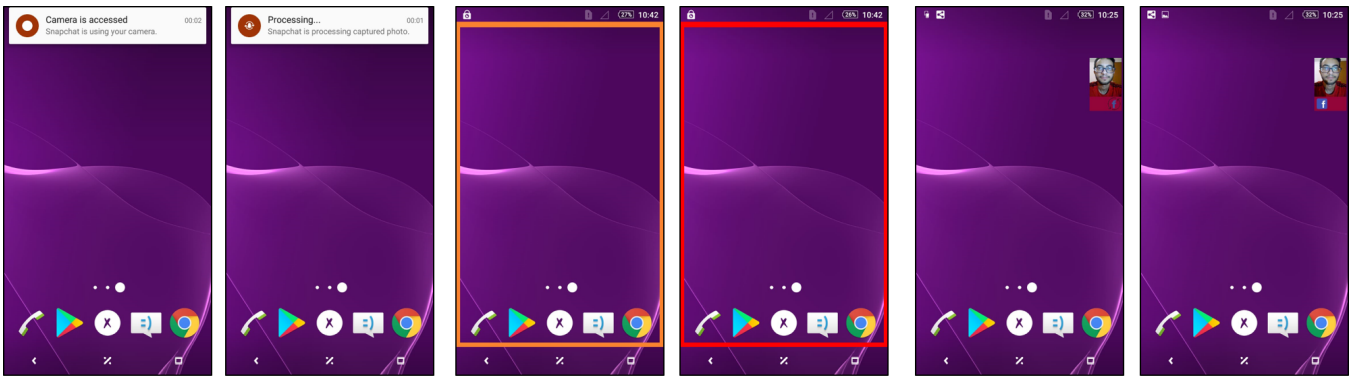

Figure 2: Concept Implementation: (A) notification nudges (access/processing), (B) Frame nudges (access/processing), and (C) Camera-preview nudges (access/processing)

proposed using the different corners of the screen to differentiate between camera states (right or left camera view). Three participants proposed using LED colours. In particular, P1 suggested using a lighting bumper and P3 proposed using a continuous LED signal when screen is off and the camera is being accessed. P2 suggested adding borders to the applications' icons indicating which functions the application is capable of doing. For instance, an orange color could indicate that the app is recording the video feed, while a red one could indicate processing the video feed.

4 DESIGN AND IMPLEMENTATION

To realize our concepts, we developed an Android application based on the focus group outcomes. We chose three on-screen designs to show our nudges: in the *notification bar*, as a *colored frame*, and as a *camera preview* as shown in Figure 2.

Notification Bar Nudges: they appear as heads-up notifications [5], which means they appear the moment the application issues the notification, and then disappear but remain in the notification drawer. We chose two different icons to differentiate between accessing camera and processing photos or videos. We chose to represent the camera access by a blinking recording dot, which was shown to be a well-known metaphor through our focus group. To show that photos or videos are being processed, we designed an icon which includes two rotating arrows denoting processing. According to our design space, notification bar nudges are classified as non-blocking and persistent nudges (Figure 2A).

Frame Nudges: we designed a colored border around the screen alongside an ordinary notification depicting the camera status. Inspired by Alrayes et al [3], we used different frame colors to denote different levels: an orange frame is displayed when front camera is accessed and a red frame is displayed when video feed/photos are being processed. According to our design space, frame nudges are classified as persistent and non-blocking nudges (Figure 2B).

Camera View Nudges: we designed a pop-up window consisting of two views: a camera preview and an icon of the application using the camera at the time. The pop-up window is displayed as long as front-facing camera is being accessed or video feed/photos are being processed. Camera Preview nudges are classified as persistent and semi-blocking nudges since they cover a relatively big portion of the screen (Figure 2C).

5 USER STUDY

We recruited 15 participants aged between 21 and 64 years old (M = 29.6 years, SD = 11.7 years, 6 females, 9 males) through mailing lists to evaluate the nudge designs in a lab study. While a lab study is limited in terms of ecological validity, it allowed us to eliminate distractions and to collect qualitative and quantitative data. The study complied with our university's ethics requirements. A within-subject design was used with two independent variables: **Nudge type**: notification, frame, camera preview, and **Modality**: Sound & vibration, sound only, vibration only, none.

After participants arrived to our lab they were asked to fill a consent form and a demographics questionnaire. The experimenter explained the purpose of the study, handed the participant an Android phone (Nexus 5 running Android 6.0.1), and asked them to sit in a quiet room in our lab to perform a reading task. The task was to read general knowledge articles on the smartphone about countries, food, and sports. Each participant went through twelve conditions (3 nudges × 4 feedback modalities). The order of conditions was counter balanced. For each condition, the participant read an article that we provided on the phone, and nudges were shown randomly 4-6 times whilst reading the article. After each condition, participants filled a questionnaire that we developed where they estimated how many nudges were displayed, how many of them were of camera access/video processing. To evaluate the different nudges, we asked participants to express their agreement on a 7-point Likert scale (1=totally disagree, 7=totally agree) to eight different statements about the nudge they were shown, as follows: ease of understanding, usefulness, annoyance, disruption, if they would like to receive it for each time the camera was accessed/video was processed, use in public settings, and if they would disable this feedback. We concluded with a semi-structured interview to collect qualitative feedback about their preferences and reaction to the different nudges. The study ran for 50 minutes per participant, and participants were rewarded with an online voucher.

5.1 Quantitative Results

We present median results for Likert scale items (1: Totally Disagree, 7: Totally Agree) regarding ease of understanding, usefulness, annoyance, interruptability, and suitability for public settings.

Scores show that *Notification* was the easiest to understand (M = 7, SD = 1.24), most helpful, and is the most suitable for use in public settings (M = 7, SD = 1.98). The *Frame* was found to cause fewest interruptions (M = 2, SD = 2.12) but was the hardest to understand (M = 4.75, SD = 1.46), whereas the *Camera* was the most annoying and caused the most interruptions (M = 3, SD = 1.94). *Camera* was rated as the most likely to be disabled (M = 3, SD = 1.96), and the worst for public settings (M = 6, SD = 2.14) The frame approach was found the least annoying (M = 3.5, SD = 2.23). In terms of perceived ease of understanding, a Friedman test revealed a significant main effect $\chi^2(2) = 12.237, p = 0.002$. Post-hoc analysis using Wilcoxon signed-rank tests with a Bonferroni correction (significance level ($p < 0.017$)) showed significant differences between *Notification* and *Camera* (Z=-2.835, p = 0.002) and between *Notification* and *Frame* (Z=-3.042, p = 0.002), but not between *Frame* and *Camera*. No other significant differences were found. All our participants indicated that they would like to receive feedback regardless if the camera was accessed, or if it was processing video feed (M = 6 for all approaches).

When looking in detail at the different feedback *modalities* for each approach, users found sound and vibration alongside *Notification* (M = 5, SD = 2.54), *Frame* (M = 5, SD = 2.05) or *Camera* (M = 5, SD = 2.05) relatively annoying. They perceived notifications with vibration only (M = 3, SD = 2.01), or without vibration (M = 3, SD = 2), as equally comfortable and usable. Frame nudges were perceived the least annoying regardless of feedback modality. However, these differences were not significant.

5.2 Qualitative Feedback

We asked participants for feedback about all the approaches and the different modalities and how they would likely use this feature. One researcher analyzed participant responses using thematic analysis.

All but one participant agreed that sound-enabled nudges, regardless of the approach (camera, frame or notifications) are annoying and disrupting, and that they would only use them in particular cases only. For example, if the application is not *trusted* by the user and if the user is currently not holding the phone. Two participants stated that the sound and vibration feedback should match the current device mode. One participant stated that he prefers the camera view approach as it is clear that it is related to camera access, unlike notifications which are received regularly from different types of apps and can lead to him ignoring them (P7). One participant stated choosing the notifications approach since it was the least distracting and does not occupy parts of the screen, additionally it can hold more detailed information (e.g. type of access, name of application) (P9). When asked how would they act upon the nudges, all of the participants stated that they will certainly check the privacy policy of that application accessing the camera. One participant said that he would point the phone away from their face, and one participant said he would delete that application.

6 DISCUSSION

6.1 Bullying users into Security?

There are ongoing discussions about the suitability of security warnings, and that "bulling users into security" does not work [21, 28]. If users are excessively warned, this could result in the "Crying Wolf" problem and might lead to users ignoring warnings. Unlike prior work [2, 26], which often asked users to act upon a certain nudge by dismissing it through a button, our nudge designs are either non-blocking or only semi-blocking (camera view nudges/notification nudges blocked a part of the screen temporarily). They also did not require action from the user, with the aim to merely nudge the user to encourage them to revisit the permission settings if desired. However, they were still perceived in some cases as annoying or interrupting. Ideally, systems would be secure and usable by design making it unnecessary to build mechanisms such as the ones we propose, but achieving this requires redesigning access controls in major mobile OS, which is outside this paper's scope.

6.2 Education, Feedback or Delayed Nudging

Many of the nudging techniques for privacy on mobile devices that have been explored in the recent years focus on nudging for education (e.g., *before* an app is installed, or a password decision is made) [1, 31, 34]. In our work we designed the approaches to provide feedback in real-time during camera access. Another option is *delayed* nudging to avoid information overload during usage. This can be done by, for example, providing an end of day report with the number and applications which accessed or processed the camera feed during the day, or providing the user with the *photos* taken at these points, similar to location nudging reports [2].

6.3 Design Implications

Through our concept design and evaluation of front-facing camera nudges, we provide the following recommendations:

- Use minimal nudges (e.g., frame) for general privacy and non-minimal semi-blocking nudges (e.g., camera) for high priority nudging in sensitive contexts (e.g., in cases where multiple people are captured by the camera).
- Use sound and vibration sparsely, and match their usage to the current mobile phone setting.
- Allow users to customize application nudges depending on their perceived threat, or type of access (quick camera access vs. longer video feed processing) to avoid information overload.

7 CONCLUSION AND FUTURE WORK

In this work, we designed three privacy awareness nudges for notifying users about front-facing camera access and processing based on a focus group. We evaluated our designs in a lab study and collected feedback on the designs and modalities. Frame nudges are considered to be the least intruding, and notifications are easiest to understand. Participants found the different modalities should either be disabled (sound/vibration) or match the device settings. While we investigated the awareness mobile owner of its camera usage, future work should extend this to study the implications of other sensors (e.g., microphones) and those of the front-facing camera on the privacy of others surrounding the user.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582) and by the Royal Society of Edinburgh (RSE award number 65040).

REFERENCES

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users&Rsquo; Choices Online. *ACM Computing Survey* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. ACM, 787–796.

[3] Fatma Alrayes and Alia Abdelmoty. 2016. Towards location privacy awareness on geo-social networks. In *2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST)*. IEEE, 105–114.

[4] Android. 2020. Android Developers – Camera API. https://developer.android.com/guide/topics/media/camera. Accessed 04 May 2020.

[5] Android. 2020. Android Developers – Notifications. https://developer.android.com/guide/topics/ui/notifiers/notifications. Accessed 04 May 2020.

[6] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. Little brothers watching you: Raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 12.

[7] Tolga Çapın, Antonio Haro, Vidya Setlur, and Stephen Wilkinson. 2006. Camera-based virtual environment interaction on mobile devices. In *International Symposium on Computer and Information Sciences*. Springer, 765–773.

[8] Delphine Christin, Martin Michalak, and Matthias Hollick. 2013. Raising user awareness about privacy threats in participatory sensing applications through graphical warnings. In *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*. ACM, 445.

[9] Justin Cuaresma and I Scott MacKenzie. 2014. A comparison between tilt-input and facial tracking as input methods for mobile games. In *2014 IEEE Games Media Entertainment*. IEEE, 1–7.

[10] Yanqing Cui, Jari Kangas, Jukka Holm, and Guido Grassel. 2013. Front-camera video recordings as emotion responses to mobile photos shared within close-knit groups. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 981–990.

[11] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS âĂŹ12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. https://doi.org/10.1145/2335356.2335360

[12] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2647–2656.

[13] Anders Henrysson, Joe Marshall, and Mark Billinghurst. 2007. Experiments in 3D interaction for mobile phone AR. In *Proceedings of the 5th international conference on Computer graphics and interactive techniques in Australia and Southeast Asia*. ACM, 187–194.

[14] Markus Hettig, Eugen Kiss, Jan-Frederik Kassel, Susanne Weber, Marian Harbach, and Matthew Smith. 2013. Visualizing risk by example: demonstrating threats arising from android apps. In *Symposium on Usable Privacy and Security (SOUPS)*.

[15] iOS. 2020. Apple Developer – Requesting Authorization for Media Capture on iOS. https://developer.apple.com/documentation/avfoundation/cameras_and_media_capture/requesting_authorization_for_media_capture_on_ios. Accessed 12 February 2020.

[16] Christina Katsini, Yasmeen Abdrabou, George Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions.. In *Proceedings of the 38th Annual ACM Conference on Human Factors in Computing Systems* (Honolulu, Hawaii, USA) *(CHI '20)*. ACM, New York, NY, USA, 21. https://doi.org/10.1145/3313831.3376840

[17] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI âĂŹ13)*. Association for Computing Machinery, New York, NY, USA, 3393âĂŞ3402. https://doi.org/10.1145/2470654.2466466

[18] Mohamed Khamis, Florian Alt, and Andreas Bulling. 2018. The Past, Present, and Future of Gaze-enabled Handheld Mobile Devices: Survey and Lessons Learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Barcelona, Spain) *(MobileHCI '18)*. ACM, New York, NY, USA. https://doi.org/10.1145/3229434.3229452

[19] Mohamed Khamis, Anita Baier, Niels Henze, Florian Alt, and Andreas Bulling. 2018. Understanding Face and Eye Visibility in Front-Facing Cameras of Smartphones used in the Wild.. In *Proceedings of the 36th Annual ACM Conference on Human Factors in Computing Systems* (MontrÃĺal, QuÃĺbec, Canada) *(CHI '18)*. ACM, New York, NY, USA, 12. https://doi.org/10.1145/3152832.3173854

[20] Jennifer King. 2012. How Come I'm Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations. *Smartphones and Privacy Expectations.(March 15, 2012)* (2012).

[21] Kat Krol, Matthew Moroz, and M. Angela Sasse. 2012. Don't work. Can't work? Why it's time to rethink security warnings. In *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*. 1–8. https://doi.org/10.1109/CRISIS.2012.6378951

[22] Yinghui Li, Zhichao Cao, and Jiliang Wang. 2017. Gazture: Design and Implementation of a Gaze Based Gesture Control System on Tablets. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 74 (Sept. 2017), 17 pages. https://doi.org/10.1145/3130939

[23] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 27–41.

[24] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[25] Daniel J. McDuff, Javier Hernandez, Sarah Gontarek, and Rosalind W. Picard. 2016. COGCAM: Contact-free Measurement of Cognitive Stress During Computer Tasks with a Digital Camera. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. ACM, New York, NY, USA, 4000–4004. https://doi.org/10.1145/2858036.2858247

[26] Nicholas Micallef, Mike Just, Lynne Baillie, and Maher Alharby. 2017. Stop annoying me! An empirical investigation of the usability of app privacy notifications. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction*. 371–375.

[27] Maria Roig-Maimó, Cristina Manresa-Yee, and Javier Varona. 2016. A robust camera-based interface for mobile entertainment. *Sensors* 16, 2 (2016), 254.

[28] Angela Sasse. 2015. Scaring and Bullying People into Security Won't Work. *IEEE Security Privacy* 13, 3 (May 2015), 80–83. https://doi.org/10.1109/MSP.2015.65

[29] Paul Schmieder, John Hosking, Andrew Luxton-Reilly, and Beryl Plimmer. 2013. Thumbs up: 3D gesture input on mobile phones using the front facing camera. In *IFIP Conference on Human-Computer Interaction*. Springer, 318–336.

[30] Janice Tsai, Lorrie Faith Cranor, Alessandro Acquisti, and Christina M Fong. 2006. What's it to you? a survey of online privacy concerns and risks. *A Survey of Online Privacy Concerns and Risks (October 2006) .NET Institute Working Paper* 06-29 (2006).

[31] James Turland, Lynne Coventry, Debora Jeske, Pam Briggs, and Aad van Moorsel. 2015. Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI conference*. 193–201.

[32] Gina Venolia, John C. Tang, and Kori Inkpen. 2015. SeeSaw: I See You Saw My Video Message. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. ACM, New York, NY, USA, 244–253. https://doi.org/10.1145/2785830.2785847

[33] VysionApps. 2020. Face Changers. https://play.google.com/store/apps/details?id=com.vysionapps.face28. Accessed 12 February 2020.

[34] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 2367–2376.

[35] Ka-Ping Yee. 2005. Guidelines and strategies for secure interaction design. In *Security and Usability: Designing Secure Systems That People Can Use*, Lorrie Faith Cranor and Simson Garfinkel (Eds.). O'Reilly Media, Inc., Chapter 13, 253–280.

[36] Chungkuk Yoo, Jaemyung Shin, Inseok Hwang, and Junehwa Song. 2013. FaceLog: Capturing User's Everyday Face Using Mobile Devices. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication* (Zurich, Switzerland) *(UbiComp '13 Adjunct)*. ACM, New York, NY, USA, 163–166. https://doi.org/10.1145/2494091.2494145